Root-Cause & Containment Memo

Summary
On May 16th, 2025, an attacker successfully compromised the account radiotech1@oh.ca using a malicious OAuth app that bypassed MFA, granting access to Microsoft 365 services. PowerShell-based malware executed on RADIOLOGY-VDI-23 initiated credential theft and exfiltrated approximately 2.2 GB of sensitive data. The Security Operations Center (SOC) responded by isolating the affected endpoint and blocking the exfiltration IP.

1. Initial Compromise via Malicious OAuth App

- Log: azure/aad_signins.json
  - At 05:28:47Z, radiotech1@oh.ca signs into Microsoft Graph API with no MFA.
  - At 05:29:03Z, the same user grants OAuthConsent to HealthData Sync via redirect https://hd-sync.xyz/auth.
- Log: dns/dns_logs.csv
  - Confirms DNS resolution for hd-sync.xyz at 05:29:01Z.

Conclusion: This indicates a successful phishing or social engineering attack via malicious OAuth app that bypassed MFA and gained token-based access to the user's data.

2. Post-Exploitation Activity and Credential Theft

- Log: edr/sentinelone_alerts.csv
  - At 05:32:15Z, on RADIOLOGY-VDI-23, a high-severity alert is triggered for:
    - powershell.exe spawned by rundll32.exe
    - Running a base64-encoded command pointing to a malicious script at: http://172.105.92.31/a

  Decoded PowerShell Command:
  Downloads and runs a script from the remote IP 172.105.92.31, a known TOR exit node.

Log: firewall/proxy_fw_2025-05-16.csv

  - Shows large data transfers (~2.2GB) to 172.105.92.31 under category proxy-avoidance-and-anonymizers.

- Log: siem_notable.csv
  - Suspicious Process Chain - PowerShell child of RunDLL32
  - Critical Data Exfiltration Alert — indicates over 2GB of data exfiltrated.

Conclusion: PowerShell activity indicates credential theft and data exfiltration, likely from internal data stores or Microsoft 365 services such as SharePoint which was accessed by the compromised user.

3. Indicators of Compromise

Type	Indicator
IP Address	172.105.92.31 (TOR exit, exfiltration)
Domain	hd-sync.xyz (Malicious OAuth App)
User Account	radiotech1@oh.ca
Host	RADIOLOGY-VDI-23
File/Process	adobereaderinstaller.exe (PUA on FINANCE-PC-04)
Encoded PowerShell	powershell.exe -nop -w hidden -enc [base64]
Script URL	http://172.105.92.31/a (malicious script)

4. What Was Compromised

1. **User Account: radiotech1@oh.ca**
   - Gave access to Microsoft Graph, SharePoint, and possibly Exchange Online.
   - No MFA — critical weakness.
2. **Endpoint: RADIOLOGY-VDI-23**
   - Was used to run malicious PowerShell for credential theft and exfiltration.
3. **Corporate Data**
   - Volume of exfiltrated data (~2.2 GB) indicates access to sensitive documents, possibly patient records or internal medical data.

5. Impacted Assets

Asset	Impact Description
RADIOLOGY-VDI-23	Compromised endpoint, malware execution, exfiltration
radiotech1@oh.ca	Account compromise, OAuth abuse
Microsoft 365 (SharePoint)	Likely data theft via compromised token
Network Security Gateway	Detected TOR, but allowed traffic until SOC blocked

6. Containment Actions

- Log entry at `06:05:10Z`:`"SOC Manual Containment Action"`: Host `RADIOLOGY-VDI-23` isolated, and exfiltration IP blocked.

Decision Log

Date & Times (EDT)	Decision Point	Options Considered	Final Decision	Rationale	Action Owner
May 16 - 05:32	Isolate potentially compromised endpoint	1. Monitor only 2. Full network isolation 3. Quarantine with limited forensic access	**Isolate RADIOLOGY-VDI-23 from network**	Host involved in credential theft and suspicious PowerShell execution; containment was critical to stop exfiltration	L1 SOC Analyst, approved by SOC Shift Lead
May 16 - 05:35	Block outbound traffic	1. Allow and monitor 2. Block at firewall 3. Block and alert upstream ISP	**Block destination IP 172.105.92.31 at perimeter firewall**	Confirmed data exfiltration via anonymizing proxy; blocking limits further unauthorized data transfer	Network Security Team Lead

May 16 - 05:40	Disable affected user account (radiotech1@oh.ca)	1. Keep active for forensic investigation 2. Disable immediately 3. Reset password only	**Disable account and revoke all sessions**	Account used for OAuth grant and accessing M365 apps without MFA; necessary to prevent ongoing abuse	IAM Lead, approved by Incident Commander
May 16 - 06:45	Notify executive leadership	1. Wait for full investigation 2. Notify only CISO 3. Escalate to full executive team	**Notify CIO, CISO, and VP Clinical Operations**	Potential impact to sensitive data and need for internal alignment; transparency with leadership	CISO
May 16 - 09:30	Engage third-party IR firm	1. Handle internally 2. Engage IR consultant (MOU on file) 3. Escalate to law enforcement immediately	**Engage IR firm (BlueShield Cyber)**	Need for external forensic validation, log preservation, and reporting best practices. Ensure incident is contained.	CISO, with Legal & Privacy Office support

May 17 10:00	Draft public statement	1. No public disclosure 2. Wait for audit findings 3. Issue limited-scope statement with updates to follow	**Issue public statement by end of day May 18**	Transparency and public trust; no confirmed PHI breach but proactive communication preferred	Communications Director, approved by CISO & Legal
May 17 - 11:00	Internal staff communication and controls	1. Wait for public statement 2. Notify only Radiology dept. 3. Notify all staff with FAQ and mandatory actions	**Send all-staff memo and internal FAQ**	Reinforce security awareness, limit speculation, and initiate preventative steps (e.g., password resets)	HR Director & IT Director, approved by Incident Commander
May 17 - 14:00	Patient Notification	1. Wait for classification 2. Prepare notifications 3. Notify regulators only	**Prepare patient notifications**	>2GB exfiltrated. PHIPA requires prompt action.	Privacy Officer, Communications Director

May 17 - 15:30	IPC Regulation Letter	1. Wait for classification 2. Prepare IPC Regulation Letter 3. Notify regulators only	**Prepare IPC Regulation Letter**	Required under PHIPA s.12(3) for a notifiable breach.	Privacy Officer, Communications Director, Legal
May 18 - 08:00	Root Cause Attribution & Data Classification	1. Insider Threat 2. External Compromise 3. Defer Attribution	**External Compromise**	No MFA, OAuth Consent to suspicious site.	CSIRT Lead
May 18 - 11:00	Issue Notifications	1. Issue Notifications 2. Continue to wait for additional information 3. Take no action	**Issue Notifications and IPC Letter**	Requirement to notify at the first reasonable opportunity of theft/loss or unauthorized use or disclosure	Privacy Officer, Approved by Communications Director & Legal
May 18 - 14:45	Remediation Plan	1. Reimage VDI 2. Password, session, and MFA Reset all users 3. Both 1 & 2	**3. Reimage VDI and Reset all passwords & MFA** **Increase Password Character count to min 16** **Require mandatory MFA for all employees**	Broad Compromise, lateral movement. Restore endpoint & identity integrity. Ensure controls align with best practices (NIST)	CISO, IAM Lead, Approved by Incident Commander

Regulator Letter (IPC Ontario)

Ontario Health
500 - 525 University Avenue
Toronto, ON M5G 2L3
July 15, 2025
Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8

Subject: Notification of Privacy Breach Under PHIPA s.12(3) - Operation Nightingale

Dear Commissioner,

Pursuant to subsection 12(3) of the Personal Health Information Protection Act, 2004 (PHIPA) and section 6.3 of Ontario Regulation 329/04, Ontario Health is notifying your office of a privacy breach involving personal health information (PHI) that meets the criteria for mandatory reporting.

1. **Description of the Breach**

   On May 16, 2025, Ontario Health's Security Operations Centre (SOC) detected irregular/abnormal outbound TOR traffic from a virtual desktop in the Radiology department. In parallel, our endpoint detection systems (SentinelOne) flagged a credential theft attempt involving suspicious PowerShell execution.

   Investigation confirmed that a malicious third-party application, "HealthData Sync," had been granted OAuth consent by a staff members' account (radiotech1@oh.ca) without multi-factor authentication. This unauthorized access enabled the attacker to access internal systems and exfiltrate approximately 2.2 GB of data through anonymized channels.

2. **Date of Discovery**

   The breach was detected and confirmed on May 16, 2025, at approximately 05:32 EDT. Containment actions were initiated immediately.

3. **Scope of the Breach**

   The breach potentially involved access to internal documents, diagnostic imaging records, and other files containing PHI. Affected systems were isolated, and an audit is ongoing to determine the scope of exposure. While there is no evidence of compromise to patient care systems, the volume and nature of the exfiltrated data meet the threshold for a notifiable breach under the following categories:

   - Stolen information
   - Use or disclosure without authority
   - Significant breach

4. Containment and Mitigation Measures

The following actions were immediately taken by Ontario Health:

- Isolated the affected endpoint (Radiology-VDI-23)
- Disabled the compromised user account and revoked all sessions
- Blocked TOR traffic and malicious IP addresses at the firewall
- Engaged a third-party incident response firm (BlueShield Cyber)
- Notified affected individual in accordance with PHIPA s.12(2)

5. Root Cause

The breach was attributed to an external compromise via OAuth phishing. The attacker exploited a lack of MFA enforcement and abused cloud application permissions to gain persistent access.

6. Notification to Individuals

Ontario Health began notifying affected individuals on May 18, 2025, providing details of the breach, potential risks, and recommended protective actions.

7. Remediation and Future Safeguards

Ontario Health has implemented the following corrective measures:

- Reimaged affected virtual desktops
- Enforced mandatory password resets and MFA re-enrollment for all users
- Increased password complexity requirements (minimum 16 characters)
- Enhanced monitoring of cloud app consents and endpoint behaviour
- Issued mandatory cybersecurity awareness training for all staff

Ontario Health is committed to protecting the privacy of personal health information and will continue to cooperate fully with your office. Please contact us should you require any additional information or documentation.

Sincerely,

(Name)
Chief Privacy Officer
Ontario Health

References:

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A | ontario.ca

Regulations | Information and Privacy Commissioner of Ontario

Report a privacy breach at your organization | Information and Privacy Commissioner of Ontario

Public Statement & Employee FAQ

Ontario Health – Press Statement on Security Incident

FOR IMMEDIATE RELEASE
Date: May 17, 2025

Ontario Health is actively investigating a cybersecurity incident that involved unauthorized access to one of our internal systems. The incident was identified on May 16, 2025, through proactive monitoring by our Security Operations Center (SOC), and immediate containment measures were taken to mitigate the impact.

Preliminary findings indicate that the compromise resulted from a malicious third-party application granted access to a single user account. That account was subsequently used to access internal resources and transmit data through anonymizing internet services. The affected endpoint was swiftly isolated, and the destination was blocked to prevent further data loss.

We are working closely with cybersecurity experts and relevant authorities to assess the full extent of the incident. At this time, there is no evidence to suggest that patient care systems were affected or that personal health information has been broadly compromised. However, as a precaution, we have notified impacted users and are conducting a comprehensive audit of potentially accessed data.

Ontario Health is committed to the security and privacy of the information entrusted to us. We are implementing enhanced monitoring, revising access controls, and reinforcing employee cybersecurity awareness to prevent future incidents.

We thank the public for their continued trust and will provide updates as our investigation progresses.

Media Contact:
Ontario Health Media Relations
media@ontariohealth.ca
416-555-0190

Internal Employee FAQ – Security Incident Briefing

1. What happened?
On May 16, 2025, our SOC detected unusual network activity from an internal system. Investigation confirmed that a user account was compromised through a malicious third-party app, leading to potential data exfiltration.

2. Whose account was involved?
The account of a staff member in the Radiology department was affected. The account has been disabled, and the device isolated.

3. Was patient information exposed?
There is no confirmed breach of personal health records at this time. We are reviewing all accessed data to verify impact.

4. What data was potentially accessed?
Internal documents and files that may include operational or research data. A full audit is ongoing.

5. What is being done to prevent this from happening again?
We are strengthening our MFA policies, reviewing third-party app permissions, and implementing stricter network traffic controls.

6. Do I need to take any action?
Yes. All employees are required to:

- Review their account activity
- Reset passwords
- Complete the mandatory security awareness refresher training by May 24

7. Who do I contact with concerns?
Contact the IT Security team at security@ontariohealth.ca or the Help Desk at x1000.

Operation Nightingale: Lessons Learned Summary

This section summaries the key lessons learned from the Operation Nightingale cybersecurity incident response conducted by our group.

What Went Well

- Rapid detection of anomalous activity by the Security Operations Center (SOC).
- Effective use of log correlation across EDR, DNS, Azure AD, and firewall logs
- Timely containment actions including endpoint isolation and firewall blocks
- Clear and structured decision-making documented in the Decision Log
- Professional and compliant communication with regulators, the public and internal staff

Areas for Improvement

- Initial lack of mulit-factor authentication (MFA) enforcement allowed OAuth abuse
- TOR traffic was not blocked by default, allowing exfiltration before containment
- No explicit mapping to MITRE ATT&CK techniques in the analysis workbook
- Limited visibility into third-party app consents and cloud permissions

Key Takeaways

- OAuth phishing is a growing threat vector that by-passes traditional MFA
- Endpoint behaviour monitoring and SIEM correlations are critical for early detection
- Timely and transparent communication is essential for maintaining trust
- Regulatory compliance requires precise documentation and prompt notification

Recommendations for Future Incidents

- Enforce MFA for all users and block legacy authentication protocols
- Implement default-deny policies for TOR and anonymizer traffic
- Integrate MITRE ATT&CK mapping into incident analysis workflows
- Regularly audit third-party app consents and cloud access permissions
- Conduct exercises to improve cross-functional coordination